Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

THEOREMS ON REDUCIBLE QUANTICS.

By O. E. Glenn.

§1. Introduction.

The content of §2 of the following series of theorems comprises a generalization of the Gauss-Eisenstein* theorem on the arithmetical condition for the irreducibility of a binary form in the absolute field, and some new results growing out of the principle of this generalization. We can state this theorem as follows:

A necessary condition that the binary form with integral coefficients,

$$f(x_1, x_2) = c_0x_1^m + c_1x_1^{m-1}x_2 + \cdots + c_mx_2^m,$$

all of whose coefficients except c_0 *are divisible by a prime* q*, should be reducible in the absolute field* $R(1)$ *is that*

$$c_m \equiv 0 \pmod{q^2}. \tag{1}$$

The extension of this theorem to the case of p-ary forms given in §2 is more or less direct as to the method, but the results seem of interest in themselves aside from later applications, for the criteria for reducibility become sharper as p increases. This is simply due to the fact that the number of necessary conditions corresponding to (1) is, in the general case, an increasing function of p.

In §3 we give, with certain amplifications, a new analytical theory of the linear factorability of a p-ary form. Perhaps the most unique feature of this theory is its complete generality with reference to multiple factors, and the cases where pairs of factors, though not multiple, are nevertheless not term-wise distinct. None of the theories published heretofore are general in this regard. This development leads to the important theorem that if a linearly factorable p-ary form has its leading binary form linearly reducible in a given field the p-ary form is reducible in the same field [Th. 4, 5].

In §4 some of the results of the previous sections are combined.

---

* Gauss, Disquisitiones Arithmeticæ, § 42. Eisenstein: "Ueber die Irreductibilität u. s. w. der Lemniscatengleichung." Journal für Mathem., Vol. 39, p. 160.

Königsberger, "Ueber den Eisenstein'schen Satz von Irreductibilität algebraischer Gleichungen." Journal für Mathem., Vol. 115, p. 53. See also Netto, Vorlesungen ueber Algebra, Vol. 1, p. 51.

Kronecker, "Grundzüge einer arithmetischen Theorie der algebraischen Grössen." Journal für Mathem., Vol. 92 (1882).

§2. Generalization of Eisenstein's theorem, etc.

Let us represent the general p-ary form f with integral coefficients, of order $N = m + n$, by means of the following notation:

$$(2)\qquad f_{pN} = \sum_{j_1, \dots, j_p = 0}^{N} c_{j_1 j_2 \dots j_p} x_1^{j_1} x_2^{j_2} \cdots x_p^{j_p} \quad (j_1 + j_2 + \cdots + j_p = N;\ m \geqq n),$$

no numerical factors being involved with the c's. Assume that f_{pN} is reducible in the absolute field, so that for some set of values (m, n) we will have a relation of the form

$$f_{pN} = \left(\sum_{k_1, \dots, k_p = 0}^{m} a_{k_1 k_2 \dots k_p} x_1^{k_1} x_2^{k_2} \cdots x_p^{k_p} \right) \left(\sum_{l_1, \dots, l_p = 0}^{n} b_{l_1 l_2 \dots l_p} x_1^{l_1} x_2^{l_2} \cdots x_p^{l_p} \right)$$
$$(k_1 + k_2 + \cdots + k_p = m;\ l_1 + l_2 + \cdots + l_p = n),$$

where the a's and b's are all integers.* Then

$$(3)\qquad c_{j_1 j_2 \dots j_p} = \sum_{\substack{\kappa = 0, \dots, m \\ \lambda = 0, \dots, n}} a_{\kappa_1 \kappa_2 \dots \kappa_p} b_{\lambda_1 \lambda_2 \dots \lambda_p},$$

where

$$(4)\qquad \sum_r \kappa_r = m,\ \sum_r \lambda_r = n,\ \sum_r j_r = \sum_r \kappa_r + \sum_r \lambda_r,\ j_r = \kappa_r + \lambda_r \quad (r = 1, 2, \cdots, p).$$

It is necessary to call particular attention to certain features of this notation, as the proofs of a number of theorems depend upon arithmetical properties of the bilinear expressions (3). We note first that these bilinear expressions can be written down immediately as soon as m and n are known. For the subscripts of the c's, i. e., the sets of numbers $(j_1, j_2, \cdots, j_p)$ are the partitions of N into p parts, repetitions being permitted, each part having the range 0, 1, $\cdots$, $m + n$ inclusive. Having thus written the complete set of c's we obtain the value of any one, as $c_{j_1 j_2 \cdots j_p}$, in terms of the a's and b's in the following manner: write all the partitions of j_r $(r = 1, 2, \cdots, p)$ into two parts (κ_r, λ_r), κ_r having the range 0, 1, $\cdots$, m inclusive, and λ_r the range 0, 1, $\cdots$, n inclusive. This gives all the double sets $[(\kappa_1, \kappa_2, \cdots, \kappa_p), (\lambda_1, \lambda_2, \cdots, \lambda_p)]$ which satisfy (4), and hence all of the terms of the summation on the right hand side of (3).

Secondly, with reference to two sets of p numbers $(\kappa_1, \kappa_2, \cdots, \kappa_p)$, $(\lambda_1, \lambda_2, \cdots, \lambda_p)$, we say that the sets occur in *normal order* if the set first to show, when read from right to left, a number greater than the number in the corresponding position in the other set occurs farthest to the right.

In all that follows we may (and do) assume that the terms of each bilinear expression (3) have been arranged so that the subscripts of the b's are in normal order.* Then, by virtue of (4), the subscripts of the a's occur in the exact reverse of the normal order. For convenience we also assume that the c's are arranged in a vertical column with subscripts arranged in normal order, the upper end of the column corresponding to the left hand end of a normal arrangement. There are p bilinear expressions which consist of a single term. These are

---

* If a p-ary form with integral coefficients is reducible in the absolute field into two factors, it is reducible into two factors having integral coefficients. Cf. Gauss: Loc cit., and the proof of theorem (1) below. The details of the proof of this lemma are omitted for brevity.

$$c_{\overbrace{0\ldots0}^{p-j}m+n\overbrace{0\ldots0}^{j-1}} = a_{\overbrace{0\ldots0}^{p-j}m\overbrace{0\ldots0}^{j-1}}b_{\overbrace{0\ldots0}^{p-j}n\overbrace{0\ldots0}^{j-1}} \qquad (j = p,\, p-1,\, \cdots,\, 2,\, 1) \tag{5}$$

In the above normal arrangement of the c's the first of the c's (5) ($j = p$) is the first in the column and the last ($j = 1$) is the last in the column.

Consider now a prime number q which divides $c_{00\ldots0m+n}$. It will divide a group of the c's (5) and fail to divide the rest. By a suitable re-adjustment of the notation of $x_1, \cdots, x_p$, we can bring those not divisible by q to the top of the column, that is, secure a normal arrangement of the c's such that

$$\begin{aligned}
&c_{\overbrace{0\ldots0}^{p-j}m+n\overbrace{0\ldots0}^{j-1}} \equiv 0 \pmod{q} \qquad (j = 1,\, 2,\, \cdots,\, \mu,\, \cdots,\, \mu+\nu)\\
&c_{\overbrace{0\ldots0}^{p-j}m+n\overbrace{0\ldots0}^{j-1}} \not\equiv 0 \pmod{q} \qquad (j = \mu+\nu+1,\, \mu+\nu+2,\, \cdots,\, p),
\end{aligned} \tag{6}$$

namely

$$\begin{aligned}
&c_{m+n00\ldots0} = a_{m00\ldots0}b_{n00\ldots0},\\
&c_{m+n-110\ldots0} = a_{m-110\ldots0}b_{n00\ldots0} + a_{m00\ldots0}b_{n-110\ldots0},\\
&\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\\
&c_{\overbrace{0\ldots\ldots0}^{p-\mu-\nu-1}m+n\overbrace{0\ldots0}^{\mu+\nu}} = a_{\overbrace{0\ldots\ldots0}^{p-\mu-\nu-1}m\overbrace{0\ldots0}^{\mu+\nu}}b_{\overbrace{0\ldots\ldots0}^{p-\mu-\nu-1}n\overbrace{0\ldots0}^{\mu+\nu}},\\
&\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\\
&c_{j_1j_2\ldots j_p} = \cdots\\
&\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\\
&c_{\overbrace{0\ldots0}^{p-i-1}1m+n-1\overbrace{0\ldots0}^{i-1}} = a_{\overbrace{0\ldots0}^{p-i}m\overbrace{0\ldots0}^{i-1}}b_{\overbrace{0\ldots\ldots0}^{p-i-1}1n-1\overbrace{0\ldots0}^{i-1}} + a_{\overbrace{0\ldots0}^{p-i-1}1m-1\overbrace{0\ldots0}^{i-1}}b_{\overbrace{0\ldots0}^{p-i}n\overbrace{0\ldots\ldots0}^{i-1}},\\
&c_{\overbrace{0\ldots0}^{p-i}m+n\overbrace{0\ldots0}^{i-1}} = a_{\overbrace{0\ldots0}^{p-i}m\overbrace{0\ldots0}^{i-1}}b_{\overbrace{0\ldots0}^{p-i}n\overbrace{0\ldots0}^{i-1}},\\
&\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\\
&c_{\overbrace{0\ldots0}^{p-\mu}m+n\overbrace{0\ldots0}^{\mu-1}} = a_{\overbrace{0\ldots0}^{p-\mu}m\overbrace{0\ldots0}^{\mu-1}}b_{\overbrace{0\ldots0}^{p-\mu}n\overbrace{0\ldots0}^{\mu-1}},\\
&\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\\
&c_{00\ldots0m+n} = a_{00\ldots0m}b_{00\ldots0n}.
\end{aligned} \tag{7}$$

---

[*] The b's would then be precisely in the order in which they would occur as the coefficients of a p-ary n-ic arranged according to x_1 as leading letter, x_2 as the letter next in order, etc.

Theorem I: *A set of necessary conditions that a form f, all of whose coefficients within the interval*

$$I = \{c_{\overbrace{0\ldots0}^{p-\mu}\,m+n\,\overbrace{0\ldots0}^{\mu-1}},\ \cdots,\ {}^{*}c_{\overbrace{0\ldots\ldots0}^{p-\mu-\nu-1}\,m+n\overbrace{0\ldots0}^{\mu+\nu}}\}^{*}$$

are divisible by a prime q should be reducible in the absolute field is given by

$$c_{\overbrace{0\ldots0}^{p-i}\,m+n\overbrace{0\ldots0}^{i-1}} \equiv 0\ (mod\ q^2) \quad (i = \mu, \mu+1, \cdots, \mu+\nu).$$

In proof assume [1] that, for a particular i of the set $\mu, \cdots, \mu+\nu$

$$c_{\overbrace{0\ldots0}^{p-i}\,m+n\,\overbrace{0\ldots0}^{i-1}} \not\equiv 0\ (\mathrm{mod}\ q^2).$$

Then one of the numbers

$$a_{\overbrace{0\ldots0}^{p-i}\,m\,\overbrace{0\ldots0}^{i-1}},\ b_{\overbrace{0\ldots0}^{p-i}\,n\,\overbrace{0\ldots0}^{i-1}},$$

say [2] the latter, is incongruent to zero modulo q. There is one and only one bilinear expression $(c_{j_1j_2\ldots j_p})$ which contains the term

$$a_{\overbrace{0\ldots\ldots0}^{p-\mu-\nu-1}\,m\,\overbrace{0\ldots0}^{\mu+\nu}}\,b_{\overbrace{0\ldots0}^{p-i}\,n\,\overbrace{0\ldots0}^{i-1}} (= t).$$

Since the c's and b's are arranged in normal order t is the last term in $c_{j_1\ldots j_p}$. By assumption [2] the

$$c_{\overbrace{0\ldots0}^{p-i-1}\,1\,m+n-1\,\overbrace{0\ldots0}^{i-1}}$$

in (7) gives at once from the hypothesis of he theorem

$$a_{\overbrace{0\ldots0}^{p-i-1}\,1\,m-1\,\overbrace{0\ldots0}^{i-1}} \equiv \ (\mathrm{mod}\ q).$$

By examining in turn the consecutive c's from

$$c_{\overbrace{0\ldots0}^{p-i}\,m+n\,\overbrace{0\ldots0}^{i-1}}$$

upward to $c_{j_1j_2\ldots j_p}$ we prove in the same manner that all the a's occurring in t, except

$$a_{\overbrace{0\ldots\ldots0}^{p-\mu-\nu-1}\,m\,\overbrace{0\ldots0}^{\mu+\nu}},$$

are divisible by q. Hence, since the $c_{j_1j_2\ldots j_p}$ is in I, we have

$$a_{\overbrace{0\ldots\ldots0}^{p-\mu-\nu-1}\,m\,\overbrace{0\ldots0}^{\mu+\nu}} \equiv 0\ (\mathrm{mod}\ q),$$

---

* By this notation we indicate that the starred number is not included in the interval. It only shows the upper limit of the interval.

contrary to the hypothesis of the theorem. Hence

$$c_{\overbrace{0\ldots0}^{p-i}\,m+n\,\overbrace{0\ldots0}^{i-1}} \equiv 0 \pmod{q^2}$$

or else the form f is irreducible.

Corollary 1: If $p = 2$ all of the coefficients of the form after the first are included in I, and we have Eisenstein's theorem (§ 1).

Corollary 2: If

$$c_{\overbrace{0\ldots0}^{p-i}\,m+n\,\overbrace{0\ldots0}^{i-1}} \not\equiv 0 \pmod{q^3},$$

then

$$a_{\overbrace{0\ldots0}^{p-i}\,m\,\overbrace{0\ldots0}^{i-1}} = q\alpha^{0}_{\overbrace{0\ldots0}^{p-i}\,m\,\overbrace{0\ldots0}^{i-1}}, \quad b_{\overbrace{0\ldots0}^{p-i}\,n\,\overbrace{0\ldots0}^{i-1}} = q\beta^{0}_{\overbrace{0\ldots0}^{p-i}\,n\,\overbrace{0\ldots0}^{i-1}}.\text{*}$$

Theorem 2: *If the* τ† *consecutive coefficients forming the sub-interval of* I

$$i_1 = [c_{\overbrace{0\ldots0}^{p-\mu}\,m+n\,\overbrace{0\ldots0}^{\mu-1}} = q^2\gamma^{0}_{\overbrace{0\ldots0}^{p-\mu}\,m+n\,\overbrace{0\ldots0}^{\mu-1}},\ c_{\overbrace{0\ldots0}^{p-\mu-1}\,1\,m+n-1\,\overbrace{0\ldots0}^{\mu-1}},\ \cdots]$$

are divisible by q^2 *and the remaining coefficients within the interval* I *are divisible by* q *to the first power; and if the order* $N = m + n$ *of* f *satisfies the condition*

$$(8)\quad \binom{\tfrac{1}{2}N+p-\mu-1}{p-\mu}+\binom{\tfrac{1}{2}N+p-\mu-2}{p-\mu-1}+\cdots+\binom{\tfrac{1}{2}N+p-\mu-\nu-1}{p-\mu-\nu} \geqq \tau,$$

then the order n *of a possible factor of* f *must satisfy the condition*

$$(9)\quad \binom{n+p-\mu-1}{p-\mu}+\binom{n+p-\mu-2}{p-\mu-1}+\cdots+\binom{n+p-\mu-\nu-1}{p-\mu-\nu} \geqq \tau.$$

Since

$$a_{\overbrace{0\ldots0}^{p-\mu}\,m\,\overbrace{0\ldots0}^{\mu-1}} \quad\text{and}\quad b_{\overbrace{0\ldots0}^{p-\mu}\,n\,\overbrace{0\ldots0}^{\mu-1}}$$

are, by Corollary 2, both divisible by q we can assume (that which will always be true for $\sigma = 1$ at least) that the like is true for all of the σ consecutive a numbers forming the interval

$$J = \{a_{\overbrace{0\ldots0}^{p-\mu}\,m\,\overbrace{0\ldots0}^{\mu-1}} = q\alpha^{0}_{\overbrace{0\ldots0}^{p-\mu}\,m\,\overbrace{0\ldots0}^{\mu-1}},\ a_{\overbrace{0\ldots0}^{p-\mu-1}\,1\,m-1\,\overbrace{0\ldots0}^{\mu-1}},\ \cdots\} \qquad (\sigma < \tau),$$

and of all of the σ consecutive b numbers forming the interval

$$K = \{b_{\overbrace{0\ldots0}^{p-\mu}\,n\,\overbrace{0\ldots0}^{\mu-1}} = q\beta^{0}_{\overbrace{0\ldots0}^{p-\mu}\,n\,\overbrace{0\ldots0}^{\mu-1}},\ b_{\overbrace{0\ldots0}^{p-\mu-1}\,1\,n-1\,\overbrace{0\ldots0}^{\mu-1}},\ \cdots\}.$$

---

* By a zero superscript we indicate that a number is prime to q.

† We shall refer to an interval containing τ elements as being of extent τ.

Then the σ consecutive c numbers forming the sub-interval of I

$$i_2 = \{c_{\overbrace{0\ldots0}^{p-\mu}\,m+n\,\overbrace{0\ldots0}^{\mu-1}},\ c_{\overbrace{0\ldots0}^{p-\mu-1}\,1\,m+n-1\,\overbrace{0\ldots0}^{\mu-1}},\ \cdots\}$$

have all their terms individually divisible by q^2, while the $\sigma + 1$th c, say for brevity $c_{(\sigma+1)}$, has the $\sigma + 1$th a, say $a_{(\sigma+1)}$, for a factor of its last term and the $\sigma + 1$th b, say $b_{(\sigma+1)}$, as a factor of its first term. Moreover since the b's are in normal order and the a's in the reverse order, these end terms are divisible each by q only, whereas the intermediate terms are all divisible by q^2. Thus we have after depressing the modulus by the factor q

$$a_{(\sigma+1)}\beta^{\circ} + \alpha^{\circ} b_{(\sigma+1)} \equiv 0 \pmod{q}.$$

Now there is a number c *within* the interval I which contains the term $a_{(\sigma+1)}b_{(\sigma+1)}$. Obviously also every other term of this c is divisible by q, so that we have

$$a_{(\sigma+1)}b_{(\sigma+1)} \equiv 0 \pmod{q}.$$

Hence

$$a_{(\sigma+1)} \equiv b_{(\sigma+1)} \equiv 0 \pmod{q}.$$

By repeating this argument we can increase the extent of the intervals J, K, i_2 until the extent of each is τ, provided $b_{(\tau)}$ falls within the interval formed by consecutive b's

$$L = \{b_{\overbrace{0\ldots0}^{p-\mu}\,n\,\overbrace{0\ldots0}^{\mu-1}},\ \cdots,\ {}^*b_{\overbrace{0\ldots\ldots0}^{p-\mu-\nu-1}\,n\,\overbrace{0\ldots0}^{\mu+\nu}}\}.$$

If $b_{(\tau)}$ does not we will, on the other hand, be led to the contradiction of hypothesis (6)

$$b_{\overbrace{0\ldots\ldots0}^{p-\mu-\nu-1}\,n\,\overbrace{0\ldots0}^{\mu+\nu}} \equiv 0 \pmod{q}.$$

Hence it is necessary that $b_{(\tau)}$ be contained in L. But the extent of L equals the left hand member of (9), and therefore the order n of a possible factor of f must satisfy (9).

The maximum value of n is $\frac{1}{2}N$. Hence if (8) is assumed, factors of f are possible having orders ranging from the minimum n satisfying (9) up to $\frac{1}{2}N$. This completes the proof.

Corollary 3. *If N is odd and*

$$\tau > \binom{\frac{1}{2}(N-1) + p - \mu - 1}{p - \mu} + \cdots + \binom{\frac{1}{2}(N-1) + p - \mu - \nu - 1}{p - \mu - \nu},$$

then the form f is irreducible. If N is even and

$$\tau \geqq \binom{\frac{1}{2}N + p - \mu - 1}{p - \mu} + \cdots + \binom{\frac{1}{2}N + p - \mu - \nu - 1}{p - \mu - \nu},$$

then f is irreducible unless it presents the one possible exceptional case of a form of even order N equal to the product of two forms of the same order $\frac{1}{2}N$.

In a particular case, say $N = 4$, $p = 4$, this corollary specifies an extensive class of irreducible forms, as in the following table:

μ	ν	Value τ; f irreducible unless = product of two quaternary quadratics
3	0	$\tau \geqq 2$
2	0	$\tau \geqq 3$
1	0	$\tau \geqq 4$
2	1	$\tau \geqq 5$
1	1	$\tau \geqq 7$
1	2	$\tau \geqq 9$

§ 3. **On the resolution of p-ary forms. Field of reducibility.**

If we take the product of r binary forms in as many non-homogeneous variables, viz.

$$x_i^{\nu_i} + a_1^{(i)} x_i^{\nu_i - 1} + a_2^{(i)} x_i^{\nu_i - 2} + \cdots + a_{\nu_i}^{(i)} \quad (i = 1, 2, \cdots, r),$$

and express the result in the form $\sum\limits_{j=0}^{\nu_1+\nu_2+\ldots+\nu_r} \varphi_j$, where φ_j embraces all of the terms of the product of order

$$= \nu_1 + \nu_2 + \cdots + \nu_r - j,$$

we get

$$\begin{aligned} &\prod_{k=1}^{r} x_k^{\nu_k} + \left(a_1^{(i)} \prod_{k=1}^{r} x_k x_i^{-1} + \textit{terms in } x_i \right) \prod_{k=1}^{r} x_k^{\nu_k - 1} \\ (10) \qquad &+ \left(a_2^{(i)} \prod_{k=1}^{r} x_k^2 x_i^{-2} + \textit{terms in } x_i \right) \prod_{k=1}^{r} x_k^{\nu_k - 2} + \cdots \\ &+ \left(a_{\nu_i}^{(i)} \prod_{k=1}^{r} x_k^{\nu_i} x_i^{-\nu_i} + \textit{terms in } x_i \right) \prod_{k=1}^{r} x_k^{\nu_k - \nu_i} + \varphi_{\nu_i + 1} + \cdots + \varphi_{\nu_1 + \nu_2 + \ldots + \nu_r}. \end{aligned}$$

In case ν_i is not one of the least of the orders ν, negative exponents will occur on the outside of some of the latter parentheses in this formula. When they do occur the corresponding x's with their negative exponents are to be multiplied into the terms in the parenthesis. If negative exponents still remain within the parenthesis when a general f_{r+1m} is arranged according to this formula the terms containing them are to be deleted. The leading terms will never be deleted by this process, however.

From

$$\varphi_j = \left(a_j^{(i)} \prod_{k=1}^{r} x_k^j x_i^{-j} + \textit{terms in } x_i \right) \prod_{k=1}^{r} x_k^{\nu_k - j}$$

we get at once by differentiation

$$\left\{\frac{\partial^{\nu_i-j}\varphi_j}{\partial x_i^{\nu_i-j}}\Big/\frac{\partial^{\nu_i}\varphi_0}{\partial x_i^{\nu_i}}\right\}_{x_i=0}=\frac{(\nu_i-j)\,!}{\nu_i\,!}a_j^{(i)},\quad\begin{pmatrix}j=0,1,\cdots,\nu_i\\ i=1,2,\cdots,r\end{pmatrix}. \tag{11}$$

Accordingly we have

Theorem 3: *Being given an $r+1$-ary form f known to be the product of r polynomials, the single variable in each one of which is one of the r distinct nonhomogeneous variables of the form, we can obtain the coefficients of these polynomials and therefore the polynomial factors of the form f themselves by differentiation according to formula (11). The linear factors of f are then obtained by factorization of the constituent polynomials.*

Let us now write the general ternary form f_{3m} under the notation

$$f_{3m}=x_2^m\varphi_{0\,x_1/x_2}+x_2^{m-1}\varphi_{1\,x_1/x_2}x_3+x_2^{m-2}\varphi_{2\,x_1/x_2}x_3^2+\cdots+\varphi_{m\,x_1/x_2}x_3^m,$$

where

$$\begin{aligned}x_2^{m-r}\varphi_{r\,x_1/x_2}\equiv C_{m-r,\,0,\,r}x_1^{m-r}+C_{m-r-1,\,1,\,r}x_1^{m-r-1}x_2+C_{m-r-2,\,2,\,r}x_1^{m-r-2}x_2^2\\+\cdots+C_{0m-rr}x_2^{m-r}.\end{aligned} \tag{12}$$

Assume that it is linearly factorable. Then the (x_1, x_2) terms of its factors will be furnished by the linear factors of the binary form $x_2^m\varphi_{0\,x_1/x_2}$. Let the factors of the latter be assumed to be known and let them be

$$x_1+r_ix_2\qquad(i=1,2,\cdots,t)\,(c_{m00}=1)^*$$

where $x_1+r_ix_2$ is of multiplicity α_i, and $\alpha_1+\alpha_2+\cdots+\alpha_t=m$.

Corollary 4: *The ternary form f_{3m} can be factored into factors of the respective orders $\alpha_1, \alpha_2, \cdots, \alpha_t$, which are rational and integral in the coefficients of the form f_{3m} itself on the one hand, and in the quantities r_i on the other, linear in the coefficients; according to the formula,*†

$$\begin{aligned}f_{3m}=\prod_{i=1}^{t}\Big[\frac{\partial^{\alpha_i}\varphi_{0-r_i}}{\partial r_i^{\alpha_i}}x^{\alpha_i}-\alpha_i\frac{\partial^{\alpha_i-1}\varphi_{1-r_i}}{\partial r_i^{\alpha_i-1}}x^{\alpha_i-1}y_i+\alpha_i(\alpha_i-1)\frac{\partial^{\alpha_i-2}\varphi_{2-r_i}}{\partial r_i^{\alpha_i-2}}x^{\alpha_i-2}y_i^2-\cdots\\+(-1)^{\alpha_i}\alpha_i\,!\,\varphi_{\alpha_i-r_i}y_i^{\alpha_i}\Big],\quad x_1+r_ix_2/x_3=\frac{x}{y_i}\quad(i=1,2,\cdots,t).\end{aligned} \tag{13}$$

To prove this we observe that if we multiply together the members of the group of α_i assumed factors of f_{3m}

$$x_1+r_ix_2+s_{ij}x_3\qquad(j=1,2,\cdots,\alpha_i),$$

---

* This implies that the term x_1^m certainly occurs. It may be necessary to transform f_{3m} linearly to secure this.

† A constant factor has been neglected on the left to secure symmetry. See proof of corollary below.

and in the result set

$$x_1 + r_i x_2 / x_3 = x / y_i \qquad (i = 1, 2, \cdots, t),$$

we get t binary forms

$$x^{\alpha_i} + a_1^{(i)} x^{\alpha_i - 1} y_i + \cdots + a_{\alpha_i}^{(i)} y_i^{\alpha_i} \qquad (i = 1, 2, \cdots, t).$$

Hence f_{3m} is the product of t binary forms and is a case of f in theorem (3). Hence corollary 4 follows directly from (11) when we put $\nu_i = \alpha_i$, $x_i = x / y_i$, $\varphi_j = \varphi_{j\, x_1/x_2}$, $r = t$, and notice that when $x_i = x / y_i = 0$, then $x_1 / x_2 = -r_i$.

Theorem 4: *If the leading binary form* $\varphi_{0\, x_1/x_2}$ *of a completely reducible ternary form is completely* reducible in a given field the corresponding ternary form* f_{3m} *is reducible in the same field. It is necessarily completely reducible if the factors of* $\varphi_{0\, x_1/x_2}$ *are all distinct. It may or may not be completely reducible in this field if some factors of* $\varphi_{0\, x_1/x_2}$ *are multiple.*

The terms of the general p-ary form f_{pm} [see (2)] can be arranged into the following scheme:

$$\begin{aligned} f_{pm} = {} & x_2^m \varphi_{0\, x_1/x_2} \\ & + x_2^{m-1} x_3 \varphi_{1\, x_1/x_2}^{(1)} + x_2^{m-2} x_3^2 \varphi_{2\, x_1/x_2}^{(1)} + \cdots + x_3^m \varphi_{m\, x_1/x_2}^{(1)} \\ & + x_2^{m-1} x_4 \varphi_{1\, x_1/x_2}^{(2)} + x_2^{m-2} x_4^2 \varphi_{2\, x_1/x_2}^{(2)} + \cdots + x_4^m \varphi_{m\, x_1/x_2}^{(2)} \\ & \cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot \\ & + x_2^{m-1} x_p \varphi_{1\, x_1/x_2}^{(p-2)} + x_2^{m-2} x_p^2 \varphi_{2\, x_1/x_2}^{(p-2)} + \cdots + x_p^m \varphi_{m\, x_1/x_2}^{(p-2)} \\ & + \Psi_{pm}, \end{aligned}$$

where the typical ternary form

$$\begin{aligned} X^{(j)} = {} & x_2^m \varphi_{0\, x_1/x_2} + x_2^{m-1} x_{j+2} \varphi_{1\, x_1/x_2}^{(j)} \\ & + x_2^{m-2} x_{j+2}^2 \varphi_{2\, x_1/x_2}^{(j)} + \cdots + x_{j+2}^m \varphi_{m\, x_1/x_2}^{(j)} \end{aligned} \tag{14}$$

is given by a notation analogous to (12), viz.,

$$\begin{aligned} x_2^{m-k} \varphi_{k\, x_1/x_2}^{(j)} = {} & C_{m-k0\overbrace{0\ldots0}^{j-1}k\overbrace{0\ldots0}^{p-j-2}} x_1^{m-k} + C_{m-k-11\overbrace{0\ldots}^{j-1}k\overbrace{0\ldots0}^{p-j-2}} x_1^{m-k-1} x_2 + \cdots \\ & + C_{m-k-hh\overbrace{0\ldots0}^{j-1}k\overbrace{0\ldots0}^{p-j-2}} x_1^{m-k-h} x_2^h + \cdots + C_{0m-k\overbrace{0\ldots0}^{j-1}k\overbrace{0\ldots0}^{p-j-2}} x_2^{m-k}. \end{aligned}$$

Of course Ψ_{pm} is simply the aggregate of all terms of f_{pm} which are not included in the ternary summands $X^{(j)}$.

Assume that the factors of $x_2^m \varphi_{0\, x_1/x_2}$ are $x_1 + r_i x_2$, as above, where $i = 1, 2, \cdots, t$. Then the typical form $X^{(j)}$ can be resolved by formula (13), and becomes after an unimportant numerical factor is neglected on the left

---

* We shall call a form *completely reducible* in a field when it is resolvable into linear factors in that field.

$$X^{(j)} = \prod_{i=1}^{t}\left[\frac{\partial^{\alpha_i}\varphi_{0-r_i}}{\partial r_i^{\alpha_i}}x^{\alpha_i} - \alpha_i\frac{\partial^{\alpha_i-1}\varphi_{1-r_i}{}^{(j)}}{\partial r_i^{\alpha_i-1}}x^{\alpha_i-1}y_i + \cdots + (-1)^{\alpha_i}\alpha_i\,!\varphi_{\alpha_i-r_i}{}^{(j)}y_i^{\alpha_i}\right] \tag{15}$$

$$(x_1 + r_ix_2 \,/\, x_{j+2} = x \,/\, y_i).$$

By resolving into linear factors the binary forms which constitute the rational factors of this form $X^{(j)}$ we get the coefficients r_{ij+2k} of the linear factors

$$x_1 + r_ix_2 + r_{ij+2k}x_{j+2} \qquad \begin{pmatrix} i = 1,\ 2,\ \cdots,\ t \\ k = 1,\ 2,\ \cdots,\ \alpha_i \end{pmatrix}$$

of $X^{(j)}$, and therefore the linear factors

$$x_1 + r_ix_2 + r_{i3k}x_3 + r_{i4k}x_4 + \cdots + r_{ipk}x_p \qquad \begin{pmatrix} i=1,2,\cdots,t \\ k=1,2,\cdots,\alpha_i \end{pmatrix}$$

of the form f_{pm} itself. Thus

Theorem 5: *The complete resolution of a p-ary form f_{pm} which is linearly factorable is accomplished by factoring the binary forms which constitute the rational factors of $X^{(j)}$ in* (15) $(j = 1, 2, \cdots, p - 2)$, *viz.*,

$$\frac{\partial^{\alpha_i}\varphi_{0-r_i}}{\partial r_i^{\alpha_i}}x^{\alpha_i} - \alpha_i\frac{\partial^{\alpha_i-1}\varphi_{1-r_i}{}^{(j)}}{\partial r_i^{\alpha_i-1}}x^{\alpha_i-1}y_i + \cdots + (-1)^{\alpha_i}\alpha_i!\varphi_{\alpha_i-r_i}{}^{(j)}y_i^{\alpha_i} \tag{16}$$

$$(i = 1, 2, \cdots, t).$$

One obtains the field of complete reducibility of f_{pm} by adjoining the $(p-2)t+1$ respective fields of $\varphi_{0\,x_1/x_2}$ and the forms (16).

§ 4. Further necessary conditions for reducibility in the field $R(1)$.

Theorem 6: *Let f_{3m} be a completely reducible ternary form having integral coefficients, and let the factors of $\varphi_{0\,x_1/x_2}$ be $x_1 + r_ix_2$ $(i = 1, 2, \cdots, t)$, where $x_1+r_ix_2$ is of multiplicity α_i, and r_i belongs to the field $R(1)$. Then if for some prime q and some value of i*

$$\frac{1}{\alpha_i!}\frac{\partial^{\alpha_i}\varphi_{0-r_i}}{\partial r_i^{\alpha_i}} \not\equiv 0 \pmod q, \tag{17}$$

$$\frac{1}{(\alpha_i - k)\,!}\frac{\partial^{\alpha_i-k}\varphi_{k-r_i}}{\partial r_i^{\alpha_i-k}} \equiv 0 \pmod q \qquad (k = 1, 2, \cdots, \alpha_i), \tag{18}$$

a necessary condition that f_{3m} be reducible in the absolute field further than is indicated by formula (13) *and theorem* 4 *is that*

$$\varphi_{\alpha_i-r_i} \equiv 0 \pmod{q^2}. \tag{19}$$

A set of t necessary conditions that f_{3m} be completely reducible in the absolute field is given by (19) *when $i = 1, 2, \cdots, t$.*

Referring to the typical factor in (13),

$$
\begin{aligned}
(20)\quad & \frac{\partial^{\alpha_i}\varphi_{0-r_i}}{\partial r_i^{\alpha_i}} x^{\alpha_i} - \alpha_i \frac{\partial^{\alpha_i-1}\varphi_{1-r_i}}{\partial r_i^{\alpha_i-1}} x^{\alpha_i-1}y + \cdots \\
& + (-1)^k\alpha_i(\alpha_i-1)\cdots(\alpha_i-k+1)\frac{\partial^{\alpha_i-k}\varphi_{k-r_i}}{\partial r_i^{\alpha_i-k}} x^{\alpha_i-k}y_i^k + \cdots \\
& + (-1)^{\alpha_i}\alpha_i\,!\varphi_{\alpha_i-r_i}y_i^{\alpha_i},
\end{aligned}
$$

we see that every term of this binary form will always be divisible by $\alpha_i\,!$. For, the coefficients in $\partial^{\alpha_i-k}\varphi_{k-r_i}/\partial r_i^{\alpha_i-k}$ that result from differentiation are, when detached,

$$
\begin{aligned}
(21)\quad & [(m-k)(m-k-1)\cdots(m-\alpha_i+1), \cdots, (\alpha_i-k+2)\cdots 4.3, \\
& (\alpha_i-k+1)\cdots 3.2,\ (\alpha_i-k)\cdots 2.1].
\end{aligned}
$$

All of these numbers are divisible by $(\alpha_i - k)\,!$, each being the product of $\alpha_i - k$ consecutive integers. Hence the general term in (20) is divisible by $\alpha_i\,!$; and this is true for $k = 0, 1, \cdots, \alpha_i$, which proves the statement. Thus the left hand members of (17), (18) are integers. Removing the factor $\alpha_i\,!$ from the binary form (20), theorem (6) follows directly from Eisenstein's theorem (§ 1).

We now consider two special cases of theorem (6):

$$
\begin{aligned}
(22)\quad & x_1^3 + 5x_1^2x_2 + 8x_1x_2^2 + 4x_2^3 + 5x_1^2x_3 + 15x_1x_2x_3 + 10x_2^2x_3 \\
& + (5\beta - \beta^2)x_1x_3^2 + (5\beta - \beta^2)x_2x_3^2,
\end{aligned}
$$

$$
\begin{aligned}
(23)\quad & x_1^4 + 6x_1^3x_2 + 13x_1^2x_2^2 + 12x_1x_2^3 + 4x_2^4 \\
& + x_1^3x_3 - x_1^2x_2x_3 - 10x_1x_2^2x_3 - 8x_2^3x_3 \\
& - 15x_1^2x_3^2 - 48x_1x_2x_3^2 - 27x_2^2x_3^2 \\
& - 9x_1x_3^3 + 27x_2x_3^3 \\
& + 54x_3^4.
\end{aligned}
$$

In (22) $\varphi_{0\,x_1/x_2}$ has a double root r but no triple root; in (23) $\varphi_{0\,x_1/x_2}$ has two pairs of double roots r_i $(i = 1, 2)$. The forms corresponding to (20) are, after the adventitious factor 2 ! is removed,

$$(24)\quad (-3r + 5)x^2 - (10r - 15)xy - [(5\beta - \beta^2)r - (5\beta - \beta^2)]\,y^2,$$

$$
\begin{aligned}
(25)\quad & (6r_i^2 - 18r_i + 13)x^2 + (3r_i^2 + 2r_i - 10)xy_i \\
& - (15r_i^2 - 48r_i + 27)y_i^2 \quad (i = 1, 2).
\end{aligned}
$$

In (24) $r = 2$, and if we take $q = 5$ the conditions of theorem (6) will be satisfied provided $\beta^2 - 5\beta \equiv 0 \pmod{5}$. This makes β a multiple of 5 and $\beta^2 - 5\beta \equiv 0 \pmod{5^2}$, so that the necessary condition expressed by the theorem is satisfied by *both terms* of $(5\beta - \beta^2)r - (5\beta - \beta^2)$ becoming divisible by q^2. We note in passing that the roots of (24) are $-\beta$, $-5 + \beta$, the factored form of (22) being

$$(x_1 + 2x_2 + \beta x_3)[x_1 + 2x_2 + (5 - \beta)x_3](x_1 + x_2).$$

In (25), taking $q = 3$, each term of

$$\varphi_{2-r_i} \equiv -15r_i^2 + 48r_i - 27$$

is divisible by q but all are not divisible by q^2. Hence, if the necessary condition $q^{-1}\varphi_{2-r_i} \equiv 0 \pmod{q}$ is satisfied, it must be satisfied, not termwise as in (24), but *as a congruence in* r_i. When it is solved as a congruence it determines the multiple root r_i of $\varphi_{0-r_i} = 0$. Solving the quadratic congruence

$$5r_i^2 - 16r_i + 9 \equiv 0 \pmod{3} \tag{26}$$

we get in reality the two roots 2, 0; but only $r_1 = 2$ can be considered, for this is the only one of the two which is a double root of $\varphi_{0-r_i} = 0$. With $r_1 = 2$, all of the conditions of the theorem are satisfied. The other double root of $\varphi_{0-r_i} = 0$ is $r_2 = 1$. The reason it does not appear as a root of (26) is that with $r_2 = 1$

$$3r_2^2 + 2r_2 - 10 \not\equiv 0 \pmod{3},$$

and then the hypotheses of the theorem (6) are not all satisfied. We note that (23) is really completely reducible in the absolute field. The roots of (25) are -3, -3 when $r_i = 2$; and 2, 3, when $r_i = 1$. The factored form is thus, by corollary (4),

$$(x_1 + 2x_2 + 3x_3)(x_1 + 2x_2 + 3x_3)(x_1 + x_2 - 2x_3)(x_1 + x_2 - 3x_3).$$

In the case of an f_{3m} completely reducible in field $R(1)$ and belonging to the case of theorem (6), we now see that when $\varphi_{0\,x_1/x_2}$ has multiple roots r_i the necessary condition

$$\varphi_{\alpha_i - r_i} \equiv 0 \pmod{q^2}$$

may be satisfied by every coefficient of $\varphi_{\alpha_i - r_i}$ being divisible by q^2, or it may be satisfied as a congruence of order $m - \alpha_i$ in r_i. We refer to the former case as being satisfied singularly, and in the latter case say the congruence is satisfied non-singularly. We have

Theorem 7: *If the necessary condition* $\varphi_{\alpha_i-r_i} \equiv 0$ (*mod* q^2) *is satisfied non-singularly the solution of this congruence determines some, and it may be all, of the multiple roots of the equation* $\varphi_{0-r_i} = 0$.

Theorem 8: *If in a completely reducible ternary form* f_{3m} *of even order* $m = 2n$, $\varphi_{0\,x_1/x_2}$ *has exactly n double roots* r_i *belonging to the absolute field, and if conditions* (28)

$$\frac{1}{2\,!}\frac{\partial^2\varphi_{0-r_i}}{\partial r_i^2} \not\equiv 0 \pmod q \qquad (q \text{ any odd prime}), \tag{27}$$

$$\frac{1}{(2-\kappa)\,!}\frac{\partial^{2-\kappa}\varphi_{\kappa-r_i}}{\partial r_i^{2-\kappa}} \equiv 0 \pmod q \qquad (\kappa = 1, 2). \tag{28}$$

are both satisfied singularly, then a necessary condition that f_{3m} *be completely reducible in the absolute field is that the congruence condition*

$$\varphi_{2-r_i} \equiv 0 \pmod{q^2}$$

be satisfied singularly.

In the product

$$\begin{aligned} f_{3m} &= \prod_{i=1}^{m}(x_1 + r_ix_2 + s_ix_3) \\ &= x_1^m + \Sigma r_1x_1^{m-1}x_2 + \Sigma r_1r_2x_1^{m-2}x_2^2 + \cdots \\ &\quad + \Sigma s_1x_1^{m-1}x_3 + \Sigma s_1r_2x_1^{m-2}x_2x_3 + \Sigma s_1r_2r_3x_1^{m-3}x_2^2x_3 + \cdots \\ &\quad + \Sigma s_1s_2x_1^{m-2}x_3^2 + \Sigma s_1s_2r_3x_1^{m-3}x_2x_3^2 + \Sigma s_1s_2r_3r_4x_1^{m-4}x_2^2x_3^2 + \cdots \\ &\quad + \cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot \\ &= x_2^m\varphi_{0\,x_1/x_2} + x_2^{m-1}x_3\varphi_{1\,x_1/x_2} + x_2^{m-2}x_3^2\varphi_{2\,x_1/x_2} + \cdots \end{aligned}$$

we have

$$r_{2\mu-1} = r_{2\mu} = \xi_\mu \qquad (\mu = 1, 2, \cdots, n).$$

Hence condition (27) may be written

$$(\xi_j-\xi_1)^2(\xi_j-\xi_2)^2\cdots(\xi_j-\xi_{j-1})^2(\xi_j-\xi_{j+1})^2\cdots(\xi_j-\xi_n)^2 \not\equiv 0 \pmod q \tag{29}$$

where $r_i = \xi_j$.

Now we can write*

$$\begin{aligned} x_2^{m-1}x_3\varphi_{1\,x_1/x_2} = \sum_{k=0}^{m-1}\sum_{\mu=1}^{n}\{s_{2\mu-1}\,[r_{2\mu}\Sigma r_1r_2 \cdots r_{2\mu-2}r_{2\mu+1} \cdots r_{k+1} \\ + \Sigma r_1r_2 \cdots r_{2\mu-2}r_{2\mu+1} \cdots r_{k+2}] + s_{2\mu}\,[r_{2\mu-1}\Sigma r_1r_2 \cdots r_{2\mu-2}r_{2\mu+1} \cdots r_{k+1} \\ + \Sigma r_1r_2 \cdots r_{2\mu-2}r_{2\mu+1} \cdots r_{k+2}]\,\}x_1^{m-k-1}x_2^kx_3. \end{aligned}$$

---

* This summation must be *defined* for $k = 0$, and 1. We of course let it stand for the first and second terms of $x_2^{m-1}x_3\varphi_1x_1/x_2$ respectively when $k = 0, 1$, i. e., $\tau_{\mu 0} = 1$, etc.

Evidently, since $r_{2\mu-1} = r_{2\mu}$ the coefficients of $s_{2\mu-1}$, $s_{2\mu}$ are equal in each term of (28), $k = 1$. Let these be $\tau_{\mu k}$ ($k = 0, 1, 2, \cdots, m-2$), and we have

$$\begin{aligned}\tau_{1k}(s_1 + s_2) + \tau_{2k}(s_3 + s_4) + \tau_{3k}(s_5 + s_6) + \cdots + \tau_{\mu k}(s_{2\mu-1}+s_{2\mu}) \\ + \cdots + \tau_{nk}(s_{m-1} + s_m) = \nu_k q.\end{aligned} \tag{30}$$

Solving a properly selected * set of n of these linear equations we get

$$s_{2\mu-1} + s_{2\mu} = \lambda_\mu q \qquad (\mu = 1, 2, \cdots, n),$$

where λ_μ is an integer if f_{3m} is completely reducible in the field $R(1)$. Hence we have

$$s_{2\mu-1} \equiv -\sigma_\mu, \quad s_{2\mu} \equiv \sigma_\mu \pmod{q}. \tag{31}$$

Using (31) in connection with the coefficients of $x_2^{m-2}x_3^2\varphi_{2\,x_1/x_2}$ successively we obtain

$$\sigma_1^2 + \sigma_2^2 + \sigma_3^2 + \cdots + \sigma_n^2 \equiv 0 \pmod{q}$$

$$\xi_1\sigma_1^2 + \xi_2\sigma_2^2 + \xi_3\sigma_3^2 + \cdots + \xi_n\sigma_n^2 \equiv 0 \pmod{q}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots,$$

and by induction

$$\xi_1^k\sigma_1^2 + \xi_2^k\sigma_2^2 + \xi_3^k\sigma_3^2 + \cdots + \xi_n^k\sigma_n^2 \equiv 0 \pmod{q} \tag{32}$$
$$(k = 0, 1, 2, \cdots, n-1, \cdots).$$

By (29) none of the ξ_j are congruent to each other. Hence the determinant of the congruences

$$\left.\begin{aligned}\sigma_1^2 + \sigma_2^2 + \sigma_3^2 + \cdots + \sigma_n^2 &\equiv 0 \\ \xi_1\sigma_1^2 + \xi_2\sigma_2^2 + \xi_3\sigma_3^2 + \cdots + \xi_n\sigma_n^2 &\equiv 0 \\ \xi_1^2\sigma_1^2 + \xi_2^2\sigma_2^2 + \xi_3^2\sigma_3^2 + \cdots + \xi_n^2\sigma_n^2 &\equiv 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots & \\ \xi_1^{n-1}\sigma_1^2 + \xi_2^{n-1}\sigma_2^2 + \xi_3^{n-1}\sigma_3^2 + \cdots + \xi_n^{n-1}\sigma_n^2 &\equiv 0\end{aligned}\right\} \pmod{q} \tag{33}$$

---

* If q happens to be a prime which divides some of the numerical factors of the coefficients in (28), $k = 1$, obtained by differentiation, the τ_{ik} ($i = 1, 2, \cdots, n$) in such a coefficient are all divisible by q and the corresponding equation (30) must be avoided in selecting n linear equations. Evidently the number of numbers

$$1, 2, 3, \cdots, m-2, m-1$$

divisible by q will be a maximum, when $q = 3$ and $m - 1 \equiv 0 \pmod{3}$. This maximum is $\frac{1}{3}(m-1)$. The least number of admissible equations (30), from which the $n = \frac{1}{2}m$ must be selected is thus $\frac{2}{3}(m-1)$, and $\frac{2}{3}(m-1) \geqq \frac{1}{2}m$ when $m \geqq 4$. Thus we always have n equations to solve for the $(s_{2\mu-1} + s_{2\mu})$. It is interesting to note that the case $m = 2$, to which the analysis above does not apply is not an exception to the theorem; which then reduces to Eisenstein's theorem for a quadratic equation.

is incongruent to zero, so that we have at once

$$\sigma_1 \equiv \sigma_2 \equiv \sigma_3 \equiv \cdots \equiv \sigma_n \equiv 0 \pmod{q}.$$

Thus every s_i is divisible by q, and every coefficient of φ_{2-r_i} by q^2, which was to be proved.

Corollary 5: *Further necessary conditions are that the congruences*

$$\varphi_{\nu-r_i} \equiv 0 \ (mod\ q^\nu) \qquad (\nu = 3, 4, \cdots, m)$$

be all satisfied singularly.

A theorem analogous to theorem 8 holds when f_{3m} is of odd order $m = 2n + 1$ and φ_{0-r} has one simple root and n double roots.

PHILADELPHIA, PA.